Annex H
Copy L
MR
7

~~TOP SECRET~~ TICOM/D-44

TRANSLATION OF A CRYPTANALYTIC REPORT BY OKM/4/SKL III ON ALLIED NAVAL CYPHERS, DATED 28/2/45, FROM FOLDER ENTITLED "RESEARCH PROGRESS 30/11/44 - 21/3/45" = TICOM DOC T. 520

Translations of reports in the same folder have already been issued as TICOM/D/12, D/15, D/18, D/20, D/34 and D/36.

TICOM
September 1945

No. of Pages: 5.

DISTRIBUTION:

British

D.D.3.
H.C.G.
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
C.C.R. (2)
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (2) (via Lt.Cdr. Manson)
G-2 (via Lt.Col.Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET (via Lt.Col.Johnson)
Col.Lewis Powell, USSTAF

TICOM

Chairman
S.A.C.
Cdr. Bacon
Lt.Col. Johnson
Major Seaman
Lt. Cdr. Manson
Capt. King
Ticom Files (4)

ADDITIONAL

S.A.C. for D.D.(C.S.A.)
S.A.C. for D.S.D.10, Admy.

CRYPTANALYTIC PROGRESS REPORT FOR SECTION III FQ,

SITUATION AS ON 28/2/45

1) Small Ships' Basic Code

A. Home Waters (COFOX)

No new findings from a cypher point of view.

B. Overseas (MEDOX)

At the beginning of January, all traffic hitherto encoded on FOXO went over to MEDOX. As the two systems are of the same type, it was quickly possible to break into MEDOX, and this has been done for almost every day since the change. The messages mainly contain weather reports, times of arrivals and sailings of caiques in the AEGEAN, as well as D/F reports, mining reports and sea-rescue traffic from the ADRIATIC.

Operational messages have not occurred in this traffic.

2) Small Ships' Basic Code. ((LOXO, FOXO, TRAXO)).

In January and February, the number of messages intercepted reached about 400 daily.

In the main, the traffic was from the following 5 areas of the CHANNEL and S.E. coasts of ENGLAND:

(i) YARMOUTH/LOWESTOFT
(ii) THAMES Estuary (HARWICH/NORE).
(iii) DOVER/RAMSGATE
(iv) PORTSMOUTH
(v) PLYMOUTH

The remaining areas produced only very slight material, with the exception of patrol vessel traffic from the FIRTH OF FORTH barrages.

The contants of the messages from the separate areas show the following characteristics:

(i) YARMOUTH/LOWESTOFT: weather reports; minesweeper services; sea rescue service.

(ii) THAMES: minesweeper service; patrol activity of ships under NCSO SOUTHEND and their reports on in-coming and out-going convoys and independent saidings.

The NORE/SCHELDE traffic has greatly diminished (having gone over in part to FLEET CODE) and contains almost exclusively position-reports from convoys, stragglers or ships joining convoys. Mine and U-boat warnings also occur.

(iii) DOVER/RAMSGATE; apart from the traffic with the French coast, there are also reports on the moving and supervision of buoys, as well as on pilot and patrol service.

(iv) PORTSMOUTH: weather-reports; convoy dispositions and position reports of convoys. Still only slight traffic with LE HAVRE.

(v) PLYMOUTH: convoy-traffic through the CHANNEL and to the BRISTOL CHANNEL.

During the two months covered by this report, the identification of place-names has been particularly successful. At the moment, more than half the place-name groups which occur are identified. A high degree of recovery was also achieved for figure-significations, partly through the assistance given by place-name identifications. The general state of cryptanalysis at the out-stations is at present good. A large part of the W/T messages are being completely solved.

3) Fleet Code

Report on the key-period 15/1 to 15/2/45 ("HAMBURG VII")

As the knowledge of this system increased with each key-period, it is now possible to submit extensive material to the parties responsible for immediate decoding and evaluation.

The W/T traffic often resembles the small ships' system; there is a noticeable division between the areas of usage. Whereas the Small Ships' Basic Code is used mainly on the East and South East Coasts of ENGLAND, the Fleet Code is used in the remaining areas. In the CHANNEL and THAMES/SCHELDE traffic both systems overlap. Furthermore, the FLEET CODE is used in the MED, partly together with MEDOX.

At present, it provided especially information on convoys and A/S activity.

The following were picked up during the above-mentioned key period:

HX 331 on 21/1
HXA 331 on 22/1
HX 333 on 31/1 and 1/2
HX 335 on 10/2
HX 336 on 14/2

SC 165 on 31/1
SC 166 on 12 and 13/2

MKS ? on 19 and 20/1
MKS 79 on 1/2
MKS 80 on 6/2
MKS 81 on 12/2

CU 53 on 15/1
CU 54A on 20/1
CU 56 on 5/2

TAM 53 on 19/1
TAM 62 on 27/1

ON 279 on 29 and 21/1
ON 280 on 23/1
ON 281 on 29/1
ON 282 on 1 and 3/2
ONA ? on 2/2
ON 283 on 6 and 8/2

OS/KMS No number given 13/2

UC 53 on 19/1
UC 54A on 28 and 29/1
UCC 56A on 10/2

ATM 41 on 18/1
ATM ? on 27/1
ATM 56 on 7/2

/In

In the case of the ATM convoys, the numbers identified in this system are 10 lower than those given in the operational evaluation report.

TBC 39 on 15/1
TBC 42 on 19/1
TBC 44 on 21/1
TBC ? on 9/2
TBC ? on 12/2

BYC ? on 29/2

WVP 44 on 22/1
WVP 56 on 7/2

VWP 56 on 5/2

VWL 41 on 14/2

The BB and MH convoys were particularly well picked up. The MH convoys were first identified by the cryptanalytic results of the Fleet Code, and simultaneously their connexion with the BB convoys was shown.

BB 1 on 23 and 24/1
BB 2 on 24 and 25/1
BB 3 on 26/1
BB 5 on 27/1
BB 7 on 29 and 30/1
BB 8 on 31/1
BB 10 on 2/2
BB 13 on 4/2
BB 14 on 5/2
BB 16 on 6 and 7/2
BB 17 on 8/2
BB 20 on 11/2

MH 1 on 23/1
MH 2 on 24/1
MH 3 on 24 and 25/1
MH 8 on 29/1
MH 9 on 30/1
MH 10 on 31/1
MH 15 on 6/2
MH 18 on 8/2
MH 19 on 9/2
MH 20 on 10/2
MH 21 on 12/2
MH 23 on 14/2
MH 24 on 14/2

The A/S formations play a particular role. Radar, Asdic, Hydrophone and Echolot are the search apparatus regularly mentioned. Special search methods are "Boxsearch" and "Scabbard" and a third has not yet been identified (2 code-groups which only appear in the following context: "Am carrying out - (ant)".) The methods of attack are: Hedgehog, Depth-charges, Attack with ATW (?), and a third which has not yet been identified; "Have attacked three times with --D".

The A/S formations are probably divided into groups which are numbered. Numbers have only occurred up to 31.

The transfer of the Section caused an unavoidable stoppage in the work. This was made good in the key-period covered by this report, so that work on the new period could follow on without any trouble.

The changes of staff effected simultaneously with the transfer of the section are still having unfavourable results on the work, as the newly allocated personnel lacks knowledge of work methods and routine.

4) Combined Assault Code.

In the last two months, further advances were made in the recovery of this code, corresponding to the amount of traffic received. The system continues to be used in the CHANNEL, especially for weather-reports.

The group-identifications necessary for reading the weather reports are passed to the BIGHT Naval D/F station as well as to the GRONINGEN and NEUMUNSTER Main Naval D/F stations. The decyphered texts are passed from there direct to the departments interested.

No traffic has occurred referring to the German ATLANTIC fortresses.

At the beginning of January, a message from COLOMBO was picked up, whose groups corresponded to those of the Combined Assault Code, and which bore the indicator group CATO. It is to be assumed that in the ASIATIC theatre of war a third edition of the Combined Assault Code is used, whose indicator-groups start with "C".

J.M.E.